Peneliti : Septi Andryana, S.Kom, MMSI., Fauziah, S.Kom, M.MSI
Abstraksi
Terjadinya pembajakan pada sistem komputer melibatkan berbagai macam aspek antara lain Keamanan dalam sistem komputer sangat berpengaruh terhadap beberapa faktor di bawah ini diantaranya adalah social engineering, security hole pada sistem operasi dan servis, keamanan Fisik,serangan pada jaringan DOS attack, serangan via aplikasi berbasis web,trojan, backdoor, rootkit, keylogger,virus, worm
Bila diterapkan pada keamanan aplikasi web, session hijacking mengacu pada pengambilalihan sebuah session aplikasi web yang ada.Aksi yang dilakukan melalui pengambilan kendali session yang dimiliki user lain setelah aksi pembajak berhasil mendapatkan ID session dari koneksi yang akan dibajak.. Tujuan yang dilakukan oleh pembajakan ini adalah untuk memperoleh ID yang dimiliki oleh user yang akan dibajaknya, dan secara otomatis user dapat dikendalikan oleh pembajak yang telah memiliki ID user yang bersangkutan dengan kata lain setiap user akan diremote oleh pembajak melalui jaringan. Serangan yang dilakukan secara otomatis akan bersifat fatal terhadap keamanan, firewall yang ada pada aplikasi yang sedang kita jalankan dan ada beberapa solusi yang diberikana dalam pencegahan sistem keamanan komputer.
Aturan-aturan yang akan dilakukan tersebut sama sekali tidak melengkapi atau mengikat suatu aplikasi. Tetapi sebaliknya, aturan-aturan ini dapat menjadi petunjuk yang berguna untuk mendesain sebuah session dan mekanisme state tracking yang berfungsi untuk menaggulangi semua keadaan yang terjadi pada system keamanan jaringan yang ada.
Kata kunci : session hijacking, session tracking, state tracking, DOS attack, trojan, firewall